SUPPORTING STATEMENT

OMB Control Number 0704-0478: Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing

A. JUSTIFICATION

1. Need for the Information Collection

DoD is revising the Defense Federal Acquisition Regulation Supplement (DFARS) to implement mandatory cyber incident reporting on unclassified networks or information systems by DoD contractors or those contractors designated as providing operationally critical support (DFARS case 2013-D018 published as an interim rules at 80 FR 51739 and 81472). DoD is required by statute to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Under the following mandatory statutory reporting requirements, DoD contractors are required to report cyber incidents to DoD:

a. *Section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 13, Reports to Department of Defense on Penetrations of Networks and Information Systems of Certain Contractors*. Requires all cleared defense contractors to report cyber incidents to DoD to include a description of the technique used, a summary of information potentially compromised and a sample of malicious software, if discovered and isolated by the contractor.

b. *Section 1632 of the NDAA for FY15, Reporting on Cyber Incidents with Respect to Networks and Information Systems of Operationally Critical Contractors*. Requires contractors designated as operationally critical contractors by DoD to report cyber incidents to include an assessment of the effect of the cyber incident on the ability of the contractor to meet the DoD contractual requirements, the technique used, a summary of information compromised, and a sample of malicious software, if discovered and isolated by the contractor.

As such, DFARS case 2013-D018 revises the currently approved information collection requirements under OMB Control Number 0704-0478 “Enhanced Safeguarding and Cyber Incident Reporting of Unclassified DoD Information within Industry” and adds burden for cloud computing services as discussed in paragraph 2, below.

2. Use of the Information

The revisions to the DFARS discussed below mandate reporting of cyber incidents on unclassified networks or information systems, within cloud computing services, and when they affect contractors designated as providing operationally critical support, as required by statute.

a. The clause at DFARS 252.204-7012 is renamed “Safeguarding Covered Defense Information and Cyber Incident Reporting” and the scope of the clause is expanded to cover the safeguarding of covered defense information and require contractors to report cyber incidents

involving this new class of information, as well as any cyber incident that may affect the ability to provide operationally critical support.

b. A new DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, is being added to require an offeror that proposes to vary from any of the security controls of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 in effect at the time the solicitation is issued to submit to the contracting officer a written explanation of how the specified security control is not applicable or an alternative control or protective measure is used to achieve equivalent protection.

c. A new provision is added at 252.239-7009, Representation of Use of Cloud Computing, that will require contractors to report that they "anticipate" or "do not anticipate" utilizing cloud computing service in performance of the resultant contract. The new representation will notify contracting officers of the applicability of the Cloud Computing requirements at 252.239-7010 on the contract.

d. A new clause 252.239-7010, Cloud Computing Services, is also being added, which will require reporting of cyber incidents that occur when DoD is purchasing cloud computing services.

These revisions to the DFARS facilitate mandatory cyber incident reporting requirements in accordance with statutory regulations. When reports are submitted, the DoD Cyber Crime Center will analyze the reported information for cyber threats and vulnerabilities in order to develop response measures as well as improve U.S. Government understanding of advanced cyber threat activity. In addition, the security requirements in NIST SP 800-171 are specifically tailored for use in protecting sensitive information residing in contractor information systems and generally reduce the burden placed on contractors by eliminating Federal-centric processes and requirements. The information provided by the offeror will inform the Department in assessing the overall risk to DoD covered defense information on unclassified contractor systems and networks.

3. Use of Information Technology

a. DoD contractors will provide their cyber incident information using the following options:

i. Complete and submit data with DoD-approved medium assurance certificates via an online web form.

ii. Download, complete and submit the Incident Report, via encrypted email using DoD-approved medium assurance certificates. (Fax may be used as an alternative.)

b. The use of technology (e.g., forms software and online access) will decrease the reporting burden on respondents. The online Incident Report standardizes data entry and allows

respondents to make data entry selections by checking appropriate boxes. The Incident Report also provides help text and other features to streamline data entry.

c. The representation on use of cloud computing services may be submitted electronically, in accordance with solicitation specific instructions.

4. Non-duplication

As a matter of policy, DoD reviews the Federal Acquisition Regulation (FAR) and DFARS to determine if adequate language already exists. There are two other OMB Control Numbers associated with cyber incident reporting; however, this information collection implements unique clauses/provisions and does not duplicate any other requirement. The two other OMB Control Numbers are summarized as follows:

a. *0704-0489, Defense Industrial Base Cyber Security/Information Assurance Cyber Incident Reporting*. This control number supports "voluntary" reporting of cyber incidents, while 0704-0478 supports reporting that is mandated under a DoD contract. Voluntary reporting could include grantees or members of industry who choose to voluntarily report incidents, and does not address the burden for reporting required by a DoD contractual agreement. OMB 0704-0489 also covers the online collection medium, a Defense Industrial Base/Information Assurance Incident Collection format, which is a database used for both voluntary reporting and reporting that is contractually mandated. While this collection request (0704-0478) requires submission of information via the same Incident Report as voluntary collections under 0704-0489 "Defense Industrial Base Cyber Security/Information Assurance Cyber Incident Reporting," the reporting for each occurs in different circumstances and will not cause duplication.

b. *0704-0490, Defense Industrial Base Voluntary Cyber Security/Information Assurance Points of Contact (POC) Information*. This control number supports the application process in order to join the program. This collection is also supported by a Privacy Impact Assessment and a System of Records Notice (SORN) for the cyber incident reporting program.

5. Burden on Small Business

The burden applied to small businesses to evaluate the effect of the cyber incident on DoD information and/or its mission is the minimum consistent with applicable laws, Executive orders, regulations, and prudent business practices.

6. Less Frequent Collection

The consequence of not collecting this data is that DoD is not able to protect information from its adversaries. Furthermore, DoD would not know the content of the data exfiltrated, the impact of the data loss to its mission, and how to develop appropriate countermeasures. DoD specialists who are most knowledgeable of the requirements and the need for the information reviewed the information collection frequency. This reporting requirement is needed to assess the impact of loss and to improve protection by better understanding the methods of loss.

7. Paperwork Reduction Act Guidelines

Collection of this information is consistent with 5 CFR 1320.5(d)(2). No special circumstances are required.

8. Consultation and Public Comments

a. This collection is consistent with the guidelines in 5 CFR 1320.6. Public comments were solicited in the *Federal Register* at 80 FR 51739 on August 26, 2015 as required by 5 CFR 1320.8(d). Six respondents made comments on the reporting burden; however, no changes are made to the burden estimate as a result of the public comments received. The comments received focus namely on the criteria that elicits reporting and only one respondent mentioned the reporting burden estimates, specifically the time required to submit a report.

The comment on the burden estimate per response suggested that four hours is several orders of magnitude less than it would take to submit a response; however, no supporting details were provided. The estimate of the burden per response is currently five hours per response and is based on the estimated amount of time it would take an information technology professional to submit a report. The respondent noted that their organization represents universities that perform mostly fundamental research, which would not require handling covered defense information and, as a result, would not trigger the requirement to report cyber incidents.

The comments addressing the criteria for the requirement to report cyber incidents, directly dispute the definition of a "cyber incident." As defined at DFARS 202.101, "Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." The comments question the inclusion of "or potentially" because this requires the contractor to report in more instances than if they only had to when an actual adverse effect was observed. The clarifier "or potentially" has been included in the DFARS definition of "cyber incident" since publication of final rule 2011-D039 in the *Federal Register* at 78 FR 69273 on November 18, 2013. The criteria for the reporting requirement must stand as it currently reads in order to ensure contractors report sooner than when they may know an actual adverse effect has occurred (within 72 hours). This reporting is imperative so that immediate action may be taken to notify the requiring activity, begin assessment of the potential damage that might have been caused by the incident, and develop a path forward to resolve the issue. Information obtained during the damage assessment could lead to programmatic changes depending of the extent of the incident.

b. DoD held a public meeting on Monday, December 14, 2015 (see notice published in the *Federal Register* at 80 FR 72712 on November 20, 2015). There were 85 registered attendees. Various topics were discussed with industry at the public meeting, such as scope, applicability, training, subcontractor flowdown, and implementation issues. Industry representatives specifically expressed to DoD, both prior to and at the public meeting, the need for additional time to implement the security requirements specified by NIST SP 800-171. The public meeting resulted in the issuance of a second interim rule (80 FR 81472) that extended the

implementation date of NIST SP 800-171 to not later than December 31, 2017, which may reduce the number of requests to vary from these security requirements (see paragraph 2.b.).

9. Gifts or Payment

The Government will provide no payment or gifts to respondents, other than remuneration of contractors in accordance with the terms of their contracts.

10. Confidentiality

This information is disclosed only to the extent consistent with statutory requirements, current regulations, and prudent business practices. The Privacy Act Statement of Records Notice (SORN) system identifier, DCIO 01, Defense Industrial Base (DIB) Cybersecurity Records, includes stipulations related to the release and disclosure of information collected. An update was published in the *Federal Register* on May 21, 2015 at 80 FR 29315 (see related OMB Control Number 0704-0490).

11. Sensitive Questions

No questions of a sensitive nature are involved. Only the minimum information to report a cyber incident is required.

12. Respondent Burden, and its Labor Costs

The DFARS revisions require additional reporting of cyber incidents by DoD contractors on unclassified networks or information systems and cloud computing services operated for or by DoD contractors. The revisions also require offerors to represent their intentions on the use of cloud computing services.

a. *252.204-7012, Safeguarding Unclassified Controlled Technical Information; 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls; and 252.239-7010, Cloud Computing Services:* DoD estimates that there are currently 10,000 cleared defense contractors and that all 10,000 may be required to report cyber incidents as a result of the changes to the DFARS.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	10,000
Responses per respondent	5
Number of responses	50,000
Hours per response	5
Estimated hours (number of responses multiplied hours per response)	250,000
Cost per hour (hourly wage) *	$64
Annual public burden (estimated hours multiplied by cost per hour)	$16,000,000

* Based on the Base General Schedule Pay Scale for 2015, GS14, Step 5 of $46.92 plus 36.25% overhead is $63.93, rounded to $64.

b. *252.239-7009, Representation of Use of Cloud Computing:* Offerors will be required to represent their intentions to utilize cloud computing services in response to all solicitations for information technology services. Anticipate approximately five minutes to determine and submit use of cloud computing representation.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	954
Responses per respondent	11
Number of responses	10,494
Hours per response	0.08
Estimated hours (number of responses multiplied hours per response)	840
Cost per hour (hourly wage) *	$38
Annual public burden (estimated hours multiplied by cost per hour)	$31,920

* Based on the Base General Schedule Pay Scale for 2015, GS-11, Step 5 of $27.86 plus 36.25% overhead is $37.96, rounded to $38 per hour).

c. *Total estimated burden for cyber reporting and cloud computing:*

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	10,954
Responses per respondent	5.5
Number of responses	60,494
Hours per response	4.15
Estimated hours (number of responses multiplied hours per response)	250,840
Cost per hour (hourly wage) ($63.93 rounded to $64)	$64
Annual public burden (estimated hours multiplied by cost per hour)	$16,053,760

13. Respondent Costs Other Than Burden Hour Costs

DoD does not estimate any burden hours apart from the hours in items 12 and 14.

14. Cost to the Federal Government

The time estimate for incident reports are based on the time it will take to log and compare to previous reporting, data querying, cross comparison and trend analysis, report

writing, and report review. We estimate the time associated with this task is 6 hours per response.

a. *252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, 252,204-7008, Compliance with Safeguarding Covered Defense Information Controls, and 252.239-7010, Cloud Computing Services:*

Cost to the Federal Government	
Total annual responses	50,000
Hours per response	6
Total hours	300,000
Cost per hour (hourly wage)	$64
Total cost	$19,200,000

b. *252.239-7009, Representation of Use of Cloud Computing:*

Cost to the Federal Government	
Total annual responses	10,494
Hours per response	0.02
Total hours	210
Cost per hour (hourly wage)	$38
Total cost	$7,980

15. Reasons for Change in Burden

This information collection updates existing collection approval by increasing the number of DoD contractors reporting as well as the associated burden hours. As a result, the total information collection public burden associated with DFARS clauses 252.204-7012, 252.204-7008, 252.239-7009, and 252.239-7010 has been changed as follows:

Adjustments	2013	2015	Change
Hours	114,713	250,840	136,127
Dollars	$4,244,381	$16,053,760	$11,787,521

16. Publication of Results

Results of this information will not be tabulated or published.

17. Non-Display of OMB Expiration Date

DoD is not requesting approval to omit display of the expiration date of OMB approval on the instrument of collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

DoD is not requesting exception to satisfy the statutory requirements.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS

Statistical methods will not be employed.